The First Internal Network Security System that Solves the Worm Problem

Submitted by: Folliard
Tuesday, 15 June 2004

Arbor Networks Announces Peakflow X 3.0;
The First Internal Network Security System that Solves the Worm Problem

Introducing Worm Vaccine and Safe Quarantine

London– 15 June 2004 – Arbor Networks®, a leading provider of internal network security systems, today announced Peakflow X 3.0, the industry's first comprehensive worm protection, detection, and mitigation solution. Based on Arbor Network's Relational Modeling technology, Peakflow X 3.0 now includes two revolutionary new features: Worm Vaccine™ and Safe Quarantine™ (patents pending). Worm Vaccine is the industry's first proactive tool that hardens networks before new vulnerabilities are published and exploited. Safe Quarantine is the industry's first zero-day detection and mitigation solution that stops worm propagation without interrupting critical business processes.

With the potential to inflict millions of dollars in damages within minutes of being released, worms are one of the most severe threats faced by network operators. Yet despite widespread deployment of firewalls and intrusion detection systems (IDSs), worms such as Sapphire, Blaster and Slammer have cost enterprises millions of dollars in damages and lost revenue.

Worms have stymied traditional perimeter security products such as Firewalls, IDSs and intrusion prevention systems (IPSs) for several reasons:

• They attack near zero-day, meaning they infect computers before virus detection, identification and patch management products can react with a signature.
• Worms mimic normal business traffic on the network, making it difficult to prevent propagation without stopping legitimate traffic
• Worms are an internal security problem, meaning they enter the network from behind the firewall, i.e. on a laptop or over a virtual private network (VPN).
Unlike any solution currently on the market today, Peakflow X provides key features to address these challenges:
Zero-day Worm Detection:
Peakflow X 3.0 detects a new worm without using a signature. Instead, Peakflow X analyses the flows and relationships between hosts on the network and identifies behavioral abnormalities. Because Peakflow X does not rely on signatures, it can detect worms the instant they hit the network, even if the worm is so new that a signature or even an advisory does not yet exist.

Safe Quarantine:
The Safe Quarantine feature uses a relational model to create a "whitelist" of legitimate traffic. In the face of a worm outbreak, Safe Quarantine leverages existing infrastructure such as firewalls and switches to block the worm traffic while preserving legitimate business connections, allowing enterprises to continue running their business and avoiding lost revenue and costly desktop and server cleanup costs.

Worm Vaccine:
Because Peakflow X's whitelist preserves legitimate business traffic, Peakflow X can respond to an exploit before a worm has even been developed. Customers can respond based on early warnings from a security advisory service, enabling proactive lockdown, even before a worm hits their network. Peakflow X also can simulate their organisation's response to a worm outbreak on a known vulnerability.

Worm Cleanup:
With today's mobile workforce, even pervasively deployed host security cannot guarantee that all machines will remain worm-free. Peakflow X will identify all infected hosts so that a security engineer can rapidly clean them and patch where appropriate.

"At BT, we are committed to providing the best security solutions to our customers that are available today," said Dave Harcourt, BT Network Security Manager "This involves not just protecting the Carrier Network and the services we provide to our customers, but also our internal network to ensure the continued smooth running of our day to day business functions. By integrating Arbor Networks' worm prevention solution, we are protecting our internal network from potentially devastating worm outbreaks."

"The internal network continues to be an Achilles' heel. Enterprise and government networks must have internal network security systems for real-time situational awareness to stop network misuse and harden internal infrastructure," said Tom Arthur, president and CEO of Arbor Networks. "Today Peakflow X has raised the bar on internal network security systems by adding proactive and zero-day worm prevention features that cut off worms before they even exist or by detecting the first infected host and stopping it in its tracks using your existing switching, firewall and routing investments."

Arbor Networks security solutions are deployed in the world's largest networks in North America, Europe and Asia. Peakflow X won the Tester's Choice Award by Secure Enterprise magazine for anomaly detection earlier this year. In a recent review, the product was cited as "….one of the most interesting boxes we've had the pleasure of test-driving in a long while."

About Arbor Networks
Arbor Networks' Peakflow is the most broadly deployed network integrity platform in the world, with over 75 customer that include leading service providers, MSOs in North America, Europe and Asia Pacific, the U.S. Department of Defense, and Fortune 500 companies. Arbor's network integrity systems protect organizations from zero-day security threats such as DDoS attacks and worms, and operational vulnerabilities such as inefficient peering and routing instability. Built upon the proven Peakflow platform, Arbor solutions provide accurate, real-time awareness of behavior across the entire network, enabling organizations to better secure and more efficiently operate their networks. Arbor is headquartered in Lexington, MA, with a research and development office in Ann Arbor, MI and EMEA headquarters in London. For more information, please visit http://www.arbornetworks.com.

registered trademarks and the Arbor Networks logo and ArbOS are trademarks of Arbor Networks, Inc. in the USA and other countries. All other trademarks are the property of their respective owners.

###

Contact:
Kate Munro
Arbor Networks
kmunro@arbor.net
+1 781.768.3253

Or

Mo Murphy
Folliard,
Murphy@folliard.co.uk
+44 (0)207 686 0625